UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/562,488	12/22/2005	Adrian Alvarez Diez	DE920030032US1	6307

30206 7590 03/11/2009

IBM CORPORATION
ROCHESTER IP LAW DEPT. 917
3605 HIGHWAY 52 NORTH
ROCHESTER, MN 55901-7829

EXAMINER	
SHAW, PETER C	
ART UNIT	PAPER NUMBER
2458	

MAIL DATE	DELIVERY MODE
03/11/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/562,488	DIEZ ET AL.	
	Examiner	Art Unit	
	PETER SHAW	2458	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 February 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-19* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-19* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *17 February 2009* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-19 are pending in this action.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

2. Claims 12-16 are rejected under 35 U.S.C. 101 because the claimed inventions are directed to non-statutory subject matter. Claims 12-16 are considered functional descriptive material because the server and client components have not been limited to hardware in the specification (*See* Specification, Pages 8-10, "definition of claimed components").

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1, 4-9, and 16-17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Xiao (US PGPUB No. 2002/0152382) [as cited in Information Disclosure Statement] in view of Applicant's Admitted Prior Art [hereinafter "AAPA"].

As per claim 1, Xiao teaches a method for validating and verifying a certificate by a client comprising:

receiving from said common database of said client system ([0088], lines 2-3, "A TIO stored on a trusted server" and "a common database" serve the same function; both store certificates and other authentication information of already validated certificates for verifying later received certificates.) at least all necessary information of a third tier server certificate being accepted as trustworthy ([0063], lines 3-5, the hash value of trusted certificates, i.e. thumbprint or fingerprint),

comparing said received at least all necessary information with a server-copy of the third tier certificate received from said third tier server system (Fig. 2, 106, comparing thumbprints),

accepting said third tier server system as to be authenticated if said at least all necessary information certificate matches said server-copy of the third tier

certificate (Fig. 2, 108, matched thumbprints; Fig. 2, 116, leads to authenticated server).

Xiao does not teach determining to accept or decline a connection to said third tier server system, i.e. validating and later verifying the certificate. AAPA teaches determining to accept or decline a connection to said third tier server system, i.e. validating ([0013], lines 9-10, Manual accept/reject is viewed to represent any form of validation that is more costly than verification.) and later verifying the certificate ([0013], lines 18-19).

At the time of invention, it would have been obvious to one of ordinary skill in the art, to combine the teachings of Xiao, with the teachings of AAPA, determining to accept or decline a connection to said third tier server system, i.e. validating and later verifying the certificate, to improve efficiency by limiting the amount of validation required.

As per claim 4, the combination of Xiao and AAPA teaches said at least all necessary information consisting essentially of a client-copy of said third tier server certificate as stored in the common data base of said distributed application environment, (Xiao, [0076], line 4, "A certified thumbprint" is all that is necessary to verify a received certificate.), and a server name which has transmitted said client-copy of said third tier server certificate to said client system (Xiao, [0098], lines 24-25, "Associated trust information" is viewed to include server name; also, it is well known in the art that a certificate, hashed or not, contains the "subject" server name.).

As per claim 5, the combination of Xiao and AAPA teaches at least all necessary information consisting essentially of a fingerprint of a client-copy of said third tier server (Xiao, [0076], line 4, "certificate thumbprint"), and a server name which has transmitted said client-copy of said third tier server certificate to said client system (Xiao, [0098], lines 24-25, "Associated trust information" is viewed to include server name; also, it is well known in the art that a certificate, hashed or not, contains the "subject" server name.).

As per claim 6, the combination of Xiao and AAPA teaches at least all necessary information consisting essentially of two different fingerprints of a client-copy of said third tier server (Xiao, [0076], line 4, "certificate thumbprint," It is implicit that the process can be performed multiple times for added security.), and a server name which has transmitted said client-copy of said third tier server certificate to said client system (Xiao, [0098], lines 24-25, "Associated trust information" includes the server name.).

As per claim 7, Xiao teaches a method comprising:

> receiving a client-copy of a third tier server certificate from a third tier server system (Fig. 2, 102),

determining whether said received client-copy of said third tier server certificate can be accepted as trustworthy (Fig. 2, 122, Validation performed by root retrieving certificate.),

storing said client-copy of said third tier server certificate in said common data base of the distributed application environment if said client-copy of said third tier server certificate has been accepted as trustworthy ([0078], line 7-8, Updating the TIO involves storing thumbprints of certificates in its table.), and

transferring to each server of said server systems at least all necessary information of said client-copy of said third tier server certificates being accepted as trustworthy ([0088], lines 2-3, The hash values in the TIO are all that are necessary to validate a certificate.)

Xiao does not teach determining to accept or decline a connection to said third tier server system, i.e. validating and later verifying the certificate. AAPA teaches determining to accept or decline a connection to said third tier server system, i.e. validating ([0013], lines 9-10, Manual accept/reject is viewed to represent any form of validation that is more costly than verification.) and later verifying the certificate ([0013], lines 18-19).

At the time of invention, it would have been obvious to one of ordinary skill in the art, to combine the teachings of Xiao, with the teachings of AAPA, determining to accept

or decline a connection to said third tier server system, i.e. validating and later verifying the certificate, to improve efficiency by limiting the amount of validation required.

As per claim 8, the combination of Xiao and AAPA teaches storing a name of said third tier server system that has transmitted said client-copy of said third tier certificate (Xiao, [0098], lines 24-25, "Associated trust information" is viewed to include server name; also, it is well known in the art that a certificate, hashed or not, contains the "subject" server name.).

As per claim 9, the combination of Xiao and AAPA teaches said client-copy of said third tier server certificate is received via a secure transmission protocol (Xiao, [0004], line 1).

As per claim 16, Xiao teaches a client system comprising:

> a connection negotiator component which, in a first computer process, receives incoming third tier server certificate via a secure connection from said third tier server ([0088], lines 2-3, "A TIO stored on a trusted server" and "a common database" serve the same function; both store certificates and other authentication information of already validated certificates for verifying later received certificates.),

a common data base of the distributed application environment which, in a second computer process, stores said third tier server certificates received from said third tier server system which have been accepted as trustworthy for the distributed application environment ([0088], lines 2-3, "A TIO stored on a trusted server" and "a common database" serve the same function; both store certificates and other authentication information of already validated certificates for verifying later received certificates.),

a certificate verifier component which, in a third computer process, compares said received third tier server certificate with information stored in said common database and stores them into said common database if it matches (Fig. 2, 106, Hashing received certificate and comparing thumbprints.),

a certificate transmitter component which, in a fifth computer process, generates certificate information of said third tier server certificates being accepted as trustworthy for determining to accept or to decline a third tier server from said common database connection ([0076], lines 3-5, Database and TIO serve the same function of holding trusted certificates in the form of hashed thumbprints)and transmits them to said application server systems via a secure ([0088], line 2, The authentication information can be sent by a trusted server to the client.).

Xiao does not teach allowing for accepting or rejecting an unknown third tier server certificate not contained in said common data base, i.e. validating and later verifying the certificate. AAPA teaches allowing for accepting or rejecting an unknown third tier server certificate not contained in said common data base, i.e. validating ([0013], lines 9-10, Manual accept/reject is viewed to represent any form of validation that is more costly than verification.) and later verifying the certificate([0013], lines 18-19).

At the time of invention, it would have been obvious to one of ordinary skill in the art, to combine the teachings of Xiao, with the teachings of AAPA, allowing for accepting or rejecting an unknown third tier server certificate not contained in said common data base, i.e. validating and later verifying the certificate, to improve efficiency by limiting the amount of validation required.

As per claim 17, the substance of the claimed invention is identical to that of claim 1. Accordingly, this claim is rejected under the same rationale.

4. Claims 2-3, 10-15, 18, and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Xiao in view of AAPA and further in view of Ramasibramani et al. (US Patent No. 6,233,577) [hereinafter "Ramasubramani"].

As per claim 2, the combination of Xiao and AAPA teaches claim 1.

The combination of Xiao and AAPA does not teach said at least all necessary receiving information from said client system is received via a non-continuous client-server connection, i.e. asynchronous connection. However, Ramasubramani teaches said at least all necessary receiving information from said client system is received via a non-continuous client-server connection, i.e. asynchronous connection (Ramasubramani, Col. 7, line 64, "receiving/sending certificates").

At the time of invention, it would have been obvious to one of ordinary skill in the art, to combine Xiao and AAPA, with the teachings of Ramasubramani, said at least all necessary receiving information from said client system is received via a non-continuous client-server connection, i.e. asynchronous connection, to allow for more flexibility as to when authentication data is to be sent or received.

As per claim 3, the newly added limitation(s) are identical to those introduced in claim 9. Accordingly, this claim is rejected under the same rationale.

As per claim 10, the newly added limitation(s) are identical to those introduced in claim 2. Accordingly, this claim is rejected under the same rationale.

As per claim 11, the combination of Xiao, AAPA, and Ramasubramani teaches authentication of said client system is accomplished by a user ID and/or password (Ramasubramani, Col. 7, lines 15-16).

As per claim 12, Xiao teaches a client system comprising:

a transfer server component, which in a first computer process, supports secure client-server connection ([0004], line 1), for receiving certificate information from a client of a third tier server certificates being accepted as trustworthy ([0063], lines 3-5, the hash value of trusted certificates, i.e. thumbprint or fingerprint)

a connection negotiator component which, in a second computer process receives incoming third tier server certificates (Fig. 2, 102) via a secure connection between said application server systems and said third tier server, ([0004], line 1)

a certificate verifier component, which in a third computer process, compares said third tier server certificate received from said third tier server with said certificate information received from client (Fig. 2, 106, comparing thumbprints).

Xiao does not teach determining to accept or decline a connection to said third tier server system, i.e. validating and later verifying the certificate. AAPA teaches determining to accept or decline a connection to said third tier server system, i.e. validating ([0013], lines 9-10, Manual accept/reject is viewed to represent any form of validation that is more costly than verification.) and later verifying the certificate ([0013], lines 18-19). At the time of invention, it would have been obvious to one of ordinary skill

in the art, to combine the teachings of Xiao, with the teachings of AAPA, determining to accept or decline a connection to said third tier server system, i.e. validating and later verifying the certificate, to improve efficiency by limiting the amount of validation required.

The combination of Xiao and AAPA does not teach a non-continuous connection, i.e. asynchronous. Ramasubramani teaches a non-continuous connection, i.e. asynchronous (Col. 7, line 64, "receiving/sending certificates"). At the time of invention, it would have been obvious to one of ordinary skill in the art to combine Xiao and AAPA, with the teachings of Ramasubramani, a non-continuous connection, i.e. asynchronous, to allow for more flexibility as to when authentication data is to be sent or received.

As per claim 13, the combination of Xiao, AAPA, and Ramasubramani, teaches certificate information comprising two different fingerprints of the original third tier server certificate (Xiao, [0076], line 4, "certificate thumbprint," It is implicit that the process can be performed multiple times for added security.), name of the server which has transmitted said third tier server certificate to said client system, and certificate name (Xiao, [0098], lines 24-25, "Associated trust information" includes the server name and certificate name.).

As per claim 14, the combination of Xiao, AAPA, and Ramasubramani teaches said two different fingerprints generated by applying two different algorithms to said third tier server certificate received from said common database (Xiao, [0098]. line 15 and 34,

"Algorithms" is recited in the plural, indicating at least two different algorithms. It is implicit that the process can be performed multiple times for added security.).

As per claim 15, the combination of Xiao, AAPA, and Ramasubramani teaches said application server systems including the same algorithms for generating the two different fingerprints (Xiao, [0098]. line 15 and 34, It is inherent that the system "includes" these algorithms.).

As per claim 18, the substance of the claim language is identical to that of claim 16. Accordingly, this claim is rejected under the same rationale.

As per claim 19, the substance of the claim language is identical to that of claim 12. Accordingly, this claim is rejected under the same rationale.

Response to Arguments

5. Applicant's arguments with respect to the claim objections have been fully considered and are persuasive. Accordingly, the objections have been withdrawn.

6. Applicant's arguments with respect to the rejections under 35 U.S.C. 112, second paragraph, have been fully considered and are persuasive. Accordingly, the rejections have been withdrawn.

7. Applicant's arguments with respect to the rejections under 35 U.S.C. 101, second paragraph, have been fully considered and are not persuasive. To be considered statutory the invention in an apparatus or system claim may not be implemented by software alone. From the examiner's understanding, the "machine test" set forth in the *Bilski* decision pertains solely to method claims. Accordingly, the rejections are maintained.

8. Applicant's arguments with respect to the prior art rejections under 35 U.S.C. 103(a) have been fully considered and are not persuasive.

In general, applicant argues that the cited prior art, Xiao and Ramasubramani, pertain to a two-tier system while the instant application pertains a third-tier system. However, the examiner submits that the applicant's admitted prior art discloses a third-tier system (AAPA; Fig. 1).

The applicant further argues that the cited prior art fails to teach the elimination of a certificate database on one side of the authentication process (AAPA; *compare* Fig. 1 *with* Fig. 2). The examiner submits that Xiao teaches a trusted third party that stores and delivers trust information to the clients (Xiao; [0088], lines 2-3, as cited above). These third parties eliminate the need for one side of the authentication exchange to maintain a database of certificates. For further clarification please see the following citation(s) (Xiao; [0050], lines 4-6, "a server based certificate management mechanism

that delivers certificates and associated trust information for clients to verify received certificates").

Accordingly, the rejections are maintained.

Conclusion

9. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to PETER SHAW whose telephone number is (571)270-7179. The examiner can normally be reached on Monday - Friday 7:30 A.M. to 5:00 P.M.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, GLENTON BURGESS can be reached on (571) 272-3949. The fax phone

number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/P. S./ February 27, 2009
Examiner, Art Unit 2458

/Joseph E. Avellino/
Primary Examiner, Art Unit 2446